(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(54) Title: METHOD FOR PROVIDING TRANSPARENT PUBLIC ADDRESSED NETWORKS WITHIN PRIVATE NETWORKS

E.G., CUSTOMER LAN   E.G., FIXED WIRELESS   E.G., PUBLIC INTERNET

FIRST NETWORK   SECOND NETWORK   THIRD NETWORK

CAN SKIP THIS STEP BECAUSE SECOND NETWORK DOES NOT REQUIRE S TO BE A 'NATIVE' ADDRESS TO FORWARD TRAFFIC TO THIRD NETWORK

D ← D'   D' ← D
S → S'   S' → S

KEY:

D= DESTINATION ADDRESS IN IP DATAGRAM
S= SOURCE ADDRESS IN IP DATAGRAM
[D,S]= GLOBALLY UNIQUE IP ADDRESSES
[D',S']= NON GLOBALLY UNIQUE IP ADDRESSES
☐ = OPTIONAL STEP

ASSUMPTIONS:

– FIRST NETWORK AND THIRD NETWORK USE GLOBALLY UNIQUE ADDRESS

– SECOND NETWORK USES NON GLOBALLY UNIQUE ADDRESSES

(57) Abstract: A system includes a first device for receiving a datagram from a public network whose destination is specified by a globally unique Internet Protocol (IP) address and for performing network address translation of said globally unique IP address to a non-globally unique IP address in a private network; and a second device for routing said datagram to a user device connected to the second device wherein said user device includes the destination specified by said non-globally unique IP address and for performing basic network address translation to said non-globally unique IP address to said corresponding globally unique IP address.

WO 01/97485 A2

METHOD FOR PROVIDING TRANSPARENT PUBLIC ADDRESSED NETWORKS WITHIN PRIVATE NETWORKS

5

FIELD OF THE INVENTION

This invention relates generally to computer network connections to the Internet or any public or private network requiring unique end station addresses and more particularly to systems and

10   techniques for passing data between public and private networks using network address translation.

BACKGROUND OF THE INVENTION

As computers become more readily available, people (users) are

15   more willing to use computers to communicate and perform their daily tasks. Typically computers are used for electronic mail, Internet access and sharing data. As computers become more prevalent, a greater number of connections to the Internet are required. Furthermore, computers are now coming in different sizes and shapes including

20   personal data assistants (PDAs), smart pagers and smart cell phones which add to the need for fast readily access to a network service provider.

In order for users using a computer to access the Internet and the World Wide Web (WWW), their computer must be connected to

25   one of the hundred or so service providers. Most service providers connect using a protocol known as the Internet Protocol (IP). The Internet Protocol uses a unique address within a computing environment to distinguish among the millions of computers connected to the Internet. An IP address is currently specified by a 32-bit host

address usually represented in dotted decimal notation (e.g.
171.10.9.4). The IP address format is now well known in the art of
computer networking. Because of the present Internet 32-bit
addressing scheme, only a total of 2^{32} (4,294,967,296) unique IP

5   addresses are possible for the entire (i.e., global or public) Internet. To
overcome this limitation, Internet service providers will typically assign
each company or organization a single IP address or in some cases a
small set of IP addresses which are unique. In addition to unique IP
addresses, certain IP addresses are reserved as non-unique IP addresses

10   to be used for private networks. These non-unique IP addresses are not
used in the public network.

In order for users to access WWW servers, and the like, IP
addresses must correctly and uniquely identify the source and target of
data packets. More specifically, IP addresses allow transmitted IP data

15   packets called datagrams, to be self-contained, independent entities of
data carrying sufficient information to be routed from the source to the
destination computer without reliance on earlier exchanges or the
transporting network. A router is a dedicated computer platform whose
sole function is to forward packets (i.e., units of transmitted data)

20   between networks. Each stub router (meaning a router that connects a
private network to a public network) executing network address
translation (NAT) features allow a non-unique IP address to be used
within a company and unique IP addresses to be used outside of the
company. The latter increases the number of computers that can be

25   connected to the Internet. The non-globally unique IP addresses can be
found in IETF RFC1918 and include 10.0.0.0 - 10.255.255.255 (a
single class A network), 172.16.0.0 - 172.31.255.255 (16 contiguous

class B networks) and 192.168.0.0 - 192.168.255.255 (256 contiguous class C networks).

As the number of private and public networks increase, the difficulty of accommodating the number of computers also increases.

5   Therefore, what is needed is a system and method for network address translation that would extend a public network across a private address network to facilitate the number of computers that can be connected to the Internet and to allow orderly topology-based routing to the computers via the private address network.

10

SUMMARY OF THE INVENTION

A system includes a first device for receiving a datagram from a public network whose destination is specified by a globally unique Internet Protocol (IP) address and for performing network address

15   translation of said globally unique IP address to a non-globally unique IP address in a private network; and a second device for routing said datagram to a user device connected to the second device wherein said user device includes the destination specified by said non-globally unique IP address and for performing basic network address translation

20   to said non-globally unique IP address to said corresponding globally unique IP address. With such an arrangement, a system is provided wherein a public network can be extended across a private address network to facilitate the number of computers that can be connected to the Internet and to facilitate orderly topology-based routing to the

25   computers via the private address network.

In accordance with a further aspect of the present invention, the second device is adapted to initially assign an IP address of the private

network to a user device and is adapted to handshake with a registration server to proxy register with an internet service provider to select an IP address of the public network and replace the IP address of the user device with the IP address of the public network. With such an

5   arrangement, datagrams from a public network can transverse a private network without the additional bandwidth required using virtual private network methodology.

In accordance with a still further aspect of the present invention, the system includes a local network connected to the user device, the

10   user device being assigned a globally unique IP addresses, the local network being assigned a set of non-unique IP addresses, a local network device adapted for performing network address translation from the local network to the corresponding public network. With such an arrangement, existing local private networks can connect to a public

15   network across a common carrier private network.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing features of this invention, as well as the invention itself, may be more fully understood from the following description of

20   the drawings in which:

FIG. 1 is a sketch of a local network connected to a private network which is connected to a public network according to the invention;

FIG. 1A is a block diagram of a local network connected to a

25   private network which is connected to a public network according to the invention;

FIG 2 is a block diagram of a computer to implement the invention;

FIG. 3 shows the layer-3 architecture and protocol stacks according to the invention;

5   FIG. 3A shows the transaction flow diagram for a new customer turning on their workstation for the first time prior to having chosen an ISP service provider;

FIG. 4. shows the transaction flow diagram for an existing customer turning on their workstation after having chosen an ISP

10   service provider;

FIG. 5 shows the transaction flow diagram for a registered user turning on their workstation after having chosen an ISP service provider; and

FIG. 6 is a sketch of a private network connected to a public

15   network which is connected to a corresponding private network according to an alternative embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

Before providing a detailed description of the invention, it may

20   be helpful to review the state of the art of Internet access within networks. In a typical private network, each workstation (computer or user device) within the private network is assigned an IP address which has only a local significance. If the number of workstations is greater than the number of globally unique IP addresses assigned to the local

25   network, which is typically the case, there must be a mapping of the locally significant IP addresses to one of the globally unique IP addresses. If a user on a first workstation initiates an outbound session

6

(e.g., HTTP, or any connection involving the exchange of datagrams),
it transmits data, for example, with a source IP address of 10.0.0.2 (i.e.,
its own locally significant IP address) and a destination IP address of
162.24.16.3 (e.g., an IP address of a target host). The stub router

5   (meaning the router that connects the private network to the public
network) maps (i.e., translates) the source IP address to one of the
organization's available globally unique IP addresses (e.g., 171.10.9.4)
before forwarding the packet to the service provider's router.

If a reply should come back (i.e., inbound), it would contain a

10   source IP address of 162.24.16.3 and a destination IP address of
171.10.9.4. The stub router would then translate the destination IP
address to 10.0.0.2 and forward the datagram to the corresponding
workstation so that the original session (and thus user) on the
workstation can receive their reply. As one skilled in the art will

15   appreciate, the stub router can correctly route subsequent reply
datagrams through the address binding, lookup and translation phases
of the particular NAT algorithm employed.

It should be appreciated that it may be desirable to connect to a
particular service provider though another network. With the

20   introduction of various new High Speed Data (HSD) Services including
wireless networks, for some computers connecting to the Internet, it
may be desirable for the computer to have a unique IP address while
connected to a network of non-unique IP addresses. For example, a
fixed wireless network may provide a user a data connection to then

25   connect to the internet service provider of the user's choice. Presently
such a connection can be implemented by first connecting the user
using DHCP with a private IP address and then making a virtual private

network (VPN) connection to a Network Access Server (NAS) to connect to the service provider which assigns a second public IP address within the VPN tunnel. Packets outbound from the user device are encapsulated with their private source address in the exterior IP

5   header and their public source address in the interior IP header. The exterior destination address of the packet is the NAS and the interior destination address is the actual destination of the packet. Packets inbound to the user device are encapsulated at the NAS to have their exterior destination address set to the private user device address and

10   their interior destination address set to the public user device IP address. One of the problems of such a technique is the additional overhead incurred in encapsulating and decapsulating the packets which reduces the effective usable bandwidth.

Referring now to Fig. 1, a network 100 includes a customer

15   network 2 connected to a private network 4 which is connected to a public network 6. The customer network 2 is connected to the private network 4 using a device 20, here a router, that operates in a manner as described further hereinafter. The private network 4 is connected to the public network 6 using a device 30, here a border router, that operates

20   in a manner as described further hereinafter. Typically, the public network 6 is used for passing a datagram (not shown) whose destination is specified by a globally unique Internet Protocol (IP) address. The public network 6 is connected to the device 30 which performs network address translation of said globally unique IP address

25   to a non-globally unique IP address in the private network 4. The second device 20 is connected to the private network 4 for routing said datagram to a user device connected to the customer network 2 wherein

said user device includes the destination specified by said non-globally unique IP address. The second device 20 performs network address translation to said non-globally unique IP address to the corresponding globally unique IP address. With such an arrangement, a technique is

5 provided wherein a public network can be extended across a private network to facilitate orderly topology-based routing to the computers via the private address network. It should soon be appreciated that such a technique provides an ability to use and transport data traffic across private address infrastructure transparent to devices in surrounding

10 public networks.

Referring now to Fig. 1A, the network 100 is shown to include a user device 10 here having assigned a global unique IP address 24.128.225.93. The user device 10 could be a stand-alone workstation or any communication device or a stub router with many private

15 workstations connected to it. The user device 10 is connected to a private network router 20. The private network router 20 is capable of performing network address translation to translate between a global unique IP address and a non-global unique IP address. The private network router 20 is connected to a second private network router 30.

20 The private network router 30 is capable of performing network address to translate between a non-global unique IP address and a global unique IP address. It should be appreciated that although the connection from private network router 20 to private network router 30 is shown as a direct connection, the connection can be accomplished

25 using any data network connectivity including multiple routers as well as fiber and radio transmission connectivity. The private network router 30 is connected to a service provider 40 which in turn is

9

connected to the Internet 50. As contemplated, the private network is using non-global unique IP addresses in a first network and the user device 10 and the service provider 40 is using a global unique IP address in a second network.

5   When the user device 10 initiates an outbound session, it transmits a datagram 10', for example, with the source IP address of 24.128.225.93 (i.e., a global unique IP address) and destination IP address of 216.41.29.6 (e.g., here an IP address assigned to another organization's network). The private network router 20 maps the source

10   IP address to one of the private network's available non-globally unique IP addresses (e.g., 10.0.0.93) before forwarding the packet to the private network. This is shown by datagram 20'. Following networking protocol within the private network, the datagram 20' arrives at private network router 30 as datagram 30' where the private network router 30

15   maps the source IP address to one of the service provider network's available globally unique IP addresses (e.g., 24.128.225.93), the IP address that was previously assigned to the user device 10, before forwarding the packet to the service provider 40. This is shown by datagram 40'. The service provider 40 then forwards the packet as

20   necessary to the Internet 50 so the packet can be delivered to its ultimate destination.

If a reply should come back (i.e., inbound) it would contain a source IP address of 216.41.29.6 and a destination IP address of 24.128.225.93. This is shown by datagram 40". The service provider

25   40 would forward the datagram 40" to the private network router 30 and the private network router 30 would then map the destination IP address to 10.0.0.93 and forward the datagram 30" to the private

network router 20 as datagram 20". The private network router 20 would then map the destination IP address to 24.128.225.93 and forward the datagram to user device 10 so that the original session (and thus user) can receive their reply. This is shown by datagram 10". The

5   above dataflow illustrates that basic address translation functionality according to the present invention. Thus, by performing network address translation at the first private network router 20 and again, in a corresponding manner, at the second private network router 30, a public network can be routed across a private network. Such a

10 technique eliminates a need for inspection and possible modification of IP datagram payload when translating addresses in the IP datagram header (sometimes referred to as application level gateways). Furthermore, this technique allows arbitrary end-to-end IP datagram encryption and authentication arrangements to inter-operate between

15 public networks separated by a shared private network.

The present invention may be implemented using hardware, software or a combination thereof and may be implemented in a computer system (for example a "router") or other processing system included within a private network's access server. In fact, in one

20 embodiment, the invention is directed toward a computer system capable of carrying out the functionality described herein. An example of a computer system 200 is shown in FIG. 2. The computer system 200 includes one or more processors, such as processor 204. The processor 204 is connected to a communication bus 206. Various

25 software embodiments are described in terms of this example computer system. After reading this description, it will become apparent to a

person skilled in the relevant art how to implement the invention using other computer systems and/or computer architectures.

Computer system 200 also includes a main memory 208, preferably random access memory (RAM), and can also include a

5   secondary memory 210. The secondary memory 210 can include, for example, a hard disk drive 212 and/or a removable storage drive 214, representing a floppy disk drive, a magnetic tape drive, an optical disk drive, etc. The removable storage drive 214 reads from and/or writes to the hard disk drive 212 in a well known manner. As will be

10   appreciated, the removable storage unit 614 includes a computer usable storage medium having stored therein computer software and/or data.

In alternative embodiments, secondary memory 210 may include other similar means for allowing computer programs or other instructions to be loaded into computer system 200. Examples of such

15   can include flash memory with a memory interface 216, a program cartridge and cartridge interface (such as that found in video game devices), a removable memory chip (such as an EPROM, or PROM) and associated socket, which allow software and data to be transferred to computer system 200. Computer system 200 can also include a

20   communications interface 218. Communications interface 218 allows software and data to be transferred between computer system 600 and external devices. Examples of communications interface 218 can include a modem, a network interface (such as an Ethernet card), a communications port, a PCMCIA slot and card, etc. Software and data

25   transferred via communications interface 218 are in the form of signals which can be electronic, electromagnetic, optical or other signals capable of being received by communications interface 218. These

12

signals are provided to communications interface 218 via a communications path (i.e., channel). This channel (not shown) carries signals and can be implemented using wire or cable, fiber optics, a phone line, a cellular phone link, an RF link and other communications

5   channels. In this description, the terms "computer program medium" and "computer usable medium" are used to generally refer to media such as removable storage drive 214, a hard disk installed in hard disk drive 212, and the like (e.g., flash memory). These computer program products are means for providing software to computer system 200.

10 Computer programs (also called computer control logic) are stored in main memory 208 and/or secondary memory 210. Computer programs can also be received via communications interface 218. Such computer programs, when executed, enable the computer system 200 to perform the features of the present invention as discussed herein. In particular,

15 the computer programs, when executed, enable the processor 204 to perform the features of the present invention. Accordingly, such computer programs represent controllers of the computer system 200.

In an embodiment where the invention is implemented using software, the software may be stored in a computer program product

20 and loaded into computer system 200 using removable storage drive 214, hard drive 212, communications interface 218 and the like (e.g., flash memory). The control logic (software), when executed by the processor 204, causes the processor 204 to perform the functions of the invention as described herein.

25 In another embodiment, the invention is implemented primarily in hardware using, for example, hardware components such as application specific integrated circuits (ASICs). Implementation of the

hardware state machine so as to perform the functions described herein will be apparent to persons skilled in the relevant art(s). In yet another embodiment, the invention is implemented using a combination of both hardware and software.

5   Referring now to Figs. 3 and 3A, a data network 100 using wireless LAN technology shall be described showing the details of how a customer or user device 10 obtains a public IP address and how a radio unit RU 20 (private network router 20) and border router (BR) 30 (private network router 30) learn the corresponding address translation

10   entries for the associated private address using the contemplated technique.

During the initial dynamic host control protocol (DHCP) handshake the user's PC or customer device 10 obtains a private IP address for use during the registration process since which ISP service

15   provider the user will use is not yet known. The RU 20 is statically provisioned with an IP address (10.0.0.1/29 in the present example) and the address of the DHCP server 32. The DHCP server 32 responds by offering the device 10 a private IP address for temporary use while the (customer) user device 10 establishes service. The customer device 10

20   next contacts the Registration Server 34 which proxy registers with a chosen ISP to establish the service. The RU 20 will allow all traffic inbound to the user device 10, using its temporary private address, to be routed to its home local area network (HLAN) since no network address translation yet exists. The ARP binding with the customer

25   device 10's physical address and private IP address is learned by the RU 20 during the DHCP exchange. When the Registration Server 34 completes the registration, it uses an SNMP SET directive to inform the

14

Service and Policy (S&P) Server 32, which in turn triggers the BR 30
to choose a public IP address from the selected ISP address pool. The
BR 30 enters the address translation entry into its Symmetric Address
Translation (SAT) table 30a. Up to this point the process is the same as

5   for the ordinary NAT registration. Now however, the BR 30 uses an
SNMP SET command to inform the S&P Server 32 of the completed
·public/private IP address binding. The S&P Server 32 in turn uses
SNMP SET command to configure its own database and the RU 20
with the same public/private SAT entry. The final step in the

10   configuration is to signal the user to reboot the customer device 10.
This is done so that the next interaction with the DHCP 32 will offer
the public address assigned from the now-registered ISP address pool
as shown in Fig. 4.

Once the user has established service, other devices, such as

15   device 12, attached to the RU 20 can obtain a public IP address in a
similar fashion as shown in Fig. 5. The primary difference in the
process is that, once the DHCP server 32 receives the DISCOVER
message and recognizes a registered customer, via the identity from the
RU 20, it does not reply with a temporary private address. Instead, the

20   S&P Server 32 informs the BR 30 of the private address, here 10.0.0.3
in the example, of the device 12 and its service policy. The BR 30 then
chooses a valid public address from the corresponding ISP address pool
and binds the public/private association into its SAT table 30a. Next
the BR 30 informs the S&P server 32 of the public/private IP binding

25   which is used to configure its internal DHCP server (not shown). The
S&P server 32 informs the RU 20 in turn of the public/private address
binding. When this is done the DHCP server 32 returns the DHCP

OFFER message with the public address to the customer device 12,
which then can begin communicating once the DHCP REQUEST/ACK
handshaking is completed, as shown in Fig. 4.

5   It should be appreciated that the technique described by which
the BR and RU some to know the public/private address bindings can
be accomplished in a variety of similar ways yielding the same results.
For example, the BR and RU could passively learn the address bindings
by inspecting the DHCP exchanges between the user device and the
DHCP server.

10   The contemplated technique, referred to herein as Symmetric
Address Translation (SAT), relies on the coordinated, symmetric use of
the IP address translation at the RU 20 and BR 30. In the unlikely
event that synchronization of SAT tables is lost or corrupted for any
reason, the user sessions will time out and be lost. This will require the

15   user devices 10 DHCP process to interact again with the internal DHCP
server of the S&P Server 32. The S&P server 32, even if it has a valid
public/private IP binding for the physical address of the requesting
device, must again interact with the BR 30 via SNMP to confirm the
binding before offering the public IP address to the user device 10. If

20   for some reason the BR 30 no longer has the same private/public
address alias binding, the S&P Server 32 will update its internal DHCP
server configuration and the RU's 20 SAT table 20a to the new binding
before offering the new public address to the device. In this way, SAT
table synchronization can be restored.

25   One attractive feature of the inventive technique will be the
ability to leverage the broadcast nature of the air interface from the
Base Stations 22 to economically 'push' content to customer device 10

16

on the Home LANs (HLANs) from servers within the network
infrastructure (e.g., the DSN). This is accomplished by using net-10 IP
broadcast to the Base Stations 22. The Base Stations 22 will in turn use
the Air Interface broadcast channel to deliver the traffic to the RU 20.

5   The RU 20 will translate the net-10 broadcast to the global broadcast
address and place it on the HLAN 14 with the broadcast physical
address so that all devices physically on the HLAN 14 can see the
traffic. IP multicasting can be used to selectively deliver content to
customer device 10, 12 with increased flexibility. The latter provides

10   the ability to broadcast or multicast to a group of unique address
devices based on a non-unique broadcast or multicast address.

It should be appreciated that one difference between typical
NAT and SAT is the customer devices 10 forming the HLAN 14 could
have disjoint public addresses as opposed to belonging to a private IP

15   address subnet. This is not as bad as it first appears since none of the
traffic between devices attached to the RU 20 would need to use the air
interface. The implication for the RU 20 is that it would have to
assume some lightweight router functionality as follows. Every device
on the RU 20 HLAN 14 would use the RU 20 as the gateway. The RU

20   20 would monitor the DHCP messages to build ARP tables for the
attached devices. If device 10 on the HLAN 14 needed to
communicate with device 12 then device 10 would ARP for the
physical address of device 12 if it determined that device 12 was on the
same subnet. Device 12 would reply to device 10 providing its

25   physical address and communication would proceed as normal. If
device 12 had an IP address that was on a different logical subnet, then
device 10 would attempt to use RU 20 as the gateway to reach device

17

12. For instance, this might happen if device 10 was registered with a
first internet service provider (ISP) ISP1 and device 12 was registered
with a second ISP, ISP2 (assuming the two ISPs provided disjoint
public address pools). The RU 20 on receiving the traffic from device

5   10 would examine its routing table and discover that device 12 was on
the same physical interface and, using its ARP table, would forward the
traffic on to device 12 after changing the physical destination address to
correspond to device 12. The RU 20 builds up the ARP table by
examining the DHCP messages between its attached clients and the

10   DHCP server. On the other hand, if the pool(s) of addresses provided
by the ISP were contiguous or subnetted so that any public address
belonging to the same IP provider would appear to be on the same
subnet. In that case device 10 would communication with device 12
without using the RU 20 as the intermediary (assuming they were

15   registered with the same ISP). Also, any attempt to reach customer
devices not on the same physical HLAN could be blocked by the RU
20 except in cases where a valid ARP entry existed in the RU 20's ARP
table. Conceivably, public addresses could be allocated in subnet
groups assigned to a particular RU. This would work by allocating a

20   small subnet of public addresses (e.g., /29) from a common pool or set
of pools of public addresses. When the customer registers their PC
(user device) with a given ISP, the subnet would be allocated to the RU
and any device attached to that RU. The customer PC (user device)
would receive one of these public addresses and a corresponding

25   private address. The BR 30 in this case would enter a subnet block of
network address entries into its table to prevent future requests from
devices on other RUs from binding to the same public addresses. Any

18

device on the same HLAN contacting the DHCP server thereafter would receive one of the public addresses in the same subnet and the RU would update its SAT table according to the number of active devices. The advantage gained by this technique would be that the

5   public addresses could be associated with a particular RU (e.g., for QoS routing within the private network infrastructure) so that SAT of outbound traffic from the RU would not be needed. However, a major disadvantage would be that ISP public addresses would have to be reserved on a per-RU basis whether or not the customer ever used

10   them. For example, a Class-B public address block could support only about 213 (8k) RU's each with /29 subnets as opposed to 2^{16} (64k) hosts in the disjoint case (i.e. potentially many more RU's if on the average each RU had only one or two attached devices on the HLAN).

The transparent nature of SAT comes from the coordinated

15   symmetric use of the address translation at the RU 20 and BR 30. For internal destinations inside the private network infrastructure (e.g., the DSN Registration Server 34) the BR 30 might not be included in the path and hence only a single SAT interface at the RU 20 would be traversed. The implication for the network is that this internal traffic

20   will require special handling. Consider the case of the customer device 10 contacting the Registration Server 34 to set up their service policy. There are two scenarios depending on whether or not the option to SAT outbound traffic at the RU 20 is used. For clarity, Unidirectional SAT will refer to the scenario where only inbound traffic is address

25   translated. Bidirectional SAT will refer to the scenario where both inbound and outbound traffic is translated.

19

In the unidirectional SAT scenario, traffic from customer devices 10 can reach any allowed internal destination including the Registration Server 34. The packets however will arrive with their public Source Address (SA). The problem then is how to route the

5   response traffic back to the customer device 10. One method is to have the internal router 24 that the Registration Server 34 is attached to, provisioned to route any public destination addresses to the exterior interface of the BR 30. The BR 30 would recognize the public address as a reachable destination within the FWS private network, address

10   translate it to the corresponding private address which then would be routed in the normal fashion to the correct RU 20. The RU 20 would address translate it back to the public address and deliver it to the customer device 10. All the advantages of SAT would apply.

Alternatively, the RU 20 could be configured to only address

15   translate outbound traffic when the destination was a private address since these would all be FWS internal destinations. The packets would then arrive at the Registration Server 34 with their private SA so that responses would be routed normally within the net-10 network. The RU 20 receiving traffic from the Registration Server 34 would network

20   address translate the traffic as usual to the correct public address and deliver the packets to the customer device 10. The disadvantage here is that there would be no simple way to support protocols that required NAT editing between the customer device 10 and internal servers. But for example, HTTP sessions could operate normally.

25   In the bidirectional SAT scenario, the RU 20 would normally address translate all outbound traffic. The packets would then arrive at the Registration Server 34 with their private SA so that responses

20

would be routed normally within the net-10 network. The RU 20
receiving traffic from the Registration Server 34 would network
address translate the traffic as usual to the correct public address and
deliver the packets to the customer device 10. Again, the only

5   disadvantage here is that there would be no simple way to support
protocols that required NAT editing between the customer device 10
and internal servers. This might not be a serious problem, for example
HTTP sessions do not require NAT editing and could operating
normally.

10   Alternatively, the RU 20 could be configured to not address
translate outbound traffic when the destination was a private address
since these would all be FWS internal destinations. Traffic from
customer devices 10 can reach any allowed internal destination
including the Registration Server 34. The packets however will arrive

15   with their public SA. The problem then is how to route the response
traffic back to the customer device 10. One method is to have the
internal router 24 that the Registration Server 34 is attached to,
provisioned to route any public destination addresses to the exterior
interface of the BR 30. The BR 30 would recognize the public address

20   as a reachable destination within the FWS network, address translate it
to the corresponding private address which then would be routed in the
normal fashion to the correct RU 20. The RU 20 would address
translate it back to the public address and deliver it to the customer
device 10. All the advantages of SAT would apply.

25   It should now be appreciated that depending upon the type of
service customers desire, the contemplated technique provides for
assigning a non-globally unique IP address when connectivity to only a

non-unique address network is desired and a unique address when connectivity to networks requiring unique addressing is desired. For example, if the customer only desires Web (HTTP) access and a HTTP Proxy Server is located in the private network, then only a non-globally

5 unique IP address is needed. If the customer wishes to connect to an ISP having a network using globally unique address, then a globally unique address can also be assigned.

Referring now to Fig. 6, a network 200 includes a private network 102 connected to a public network 104 which is connected to a

10 private network 6 using the advantages of SAT. The private networks 102, 104 use non-globally unique addresses, whereas the public network 104 uses globally unique addresses. With such an arrangement, geographically separated private networks can be connected by using the public network for communicating among the

15 private network users within the private network. The private network 102 is connected to the public network 104 using a device 120, here a router, that operates in a manner as described further hereinafter. The public network 104 is connected to the private network 106 using a device 130, here a router, that operates in a manner as described further

20 hereinafter. The private network 102 is connected to the device 120 which performs network address translation of said non-globally unique IP address to a globally unique IP address in the public network 104. The device 120 is connected to the public network 104 for routing said datagram from a user device connected to the private network 102

25 wherein said user device includes the destination specified by said non-globally unique IP address. The device 120 performs network address translation to said non-globally unique IP address to a globally unique

22

IP address. When the datagram arrives at the device 130, the device
130, using the technique of symmetric address translation, performs
network address translation to said globally unique IP address to a
corresponding non-globally unique IP address. With such an

5   arrangement, a private network can be extended across a public
network to another portion of the private network.

The network 200 is shown to include a user device 110 here
having assigned a non-global unique IP address 10.0.0.93. The user
device 110 could be a stand-alone workstation or any communication

10   device or a stub router with many private workstations connected to it.
The user device 110 is connected via the private network 102 to a
private network router 120. The private network router 120 is capable
of performing network address translation to translate between a non-
global unique IP address and a global unique IP address. The private

15   network router 120 is connected across public network 104 to a second
private network router 130. The private network router 130 is capable
of performing network address to translate between the global unique
IP address and a non-global unique IP address. It should be appreciated
that although the connection from private network router 120 to private

20   network router 130 is shown as a direct connection, the connection can
be accomplished using any data network connectivity including
multiple routers as well as fiber and radio transmission connectivity.
The private network router 130 is connected to another portion of the
private network 102, here private network 106. A user device 140 is

25   connected to the private network 106. As contemplated, the private
network 102 is using non-global unique IP addresses in a subnet
configuration to be in the same network as the private network 106.

23

Thus, user device 110 can communicate with user device 140 as though
they were on the same network. The private network router 120 and
the private network router 130 are configured with table information to
match up respective non-global unique IP addresses. As more users are
5   added to the private network, the respective SAT tables would be
passed back and forth (handshake) between the private network router
120 and the private network router 130. Using symmetric address
translation (SAT) the devices (i.e. user device 110) on the private
network 102 can communicate with the devices (i.e. user device 140)
10   on private network 106 as though they were on a contiguous single
network. It should be appreciated that a third private network (not
shown) could be added and connected to the private networks 102, 104
through the public network 104 in a similar manner.

It should now be appreciated the present invention includes a
15   first device for receiving a datagram from a public network whose
destination is specified by a globally unique Internet Protocol (IP)
address and for performing network address translation of said globally
unique IP address to a non-globally unique IP address in a private
network; and a second device for routing said datagram to a user device
20   connected to the second device wherein said user device includes the
destination specified by said non-globally unique IP address and for
performing basic network address translation to said non-globally
unique IP address to said corresponding globally unique IP address.
With such an arrangement, a system is provided wherein a public
25   network can be extended across a private network address to facilitate
the number of computers that can be connected to the Internet and to
facilitate orderly topology-based routing to the computers via the

24

private address network. Furthermore, the second device is adapted to initially assign an IP address of the private network to a user device and is adapted to handshake with a registration server to proxy register with an internet service provider to select an IP address of the public

5   network and replace the IP address of the user device with the IP address of the public network. The system further includes a local network connected to the user device, the user device being assigned a globally unique IP addresses, the local network being assigned a set of non-unique IP addresses, the user device adapted for performing

10   network address translation from the local network to the corresponding public network. With such an arrangement, existing local private networks can connect to a public network across a common carrier private network.

All publications and references cited herein are expressly

15   incorporated herein by reference in their entirety.

Having described the preferred embodiments of the invention, it will now become apparent to one of ordinary skill in the art that other embodiments incorporating their concepts may be used. It is felt therefore that these embodiments should not be limited to disclosed

20   embodiments but rather should be limited only by the spirit and scope of the appended claims.

Claims:

1.   A system comprising:

a first device for performing network address translation from a

5   first network to a second network; and

a second device for performing network address translation

from the second network to the corresponding first network.

2.   The system as recited in claim 1 wherein the first device

comprises:

10   a processor for receiving/transmitting a datagram from said first

network having a destination address with a unique IP address in the

first network and mapping said first network unique IP address to a

unique IP address in the second network; and

wherein the second device comprises:

15   a processor for mapping said second network unique IP address

to said first network unique IP address.

3.   The system as recited in claim 1 wherein:

the second device comprises a processor for receiving from a

user device having a unique IP address in the first network a datagram

20   having a source address with a non-globally unique IP address and

having a destination address with a globally unique IP address and

mapping said non-globally unique IP address of the source address to

the unique IP address of the first network and for routing said datagram

to the first network.

25   4.   The system as recited in claim 1 wherein said first network is a

public network and said second network is a private network.

26

5.   The system as recited in claim 1 wherein said first network is assigned a set of globally unique IP addresses and said second network is assigned a set of non-globally unique IP addresses.

6.   The system as recited in claim 1 further comprising:

5   a local network connected to the second device, the local network having at least one of a plurality of user devices connected via the local network, the local network being assigned a set of unique IP addresses from the first network.

7.   The system as recited in claim 6 wherein the second device,

10   with a connection to one of the plurality of computer workstations initially having an IP address of the second network, is adapted to handshake with a registration server to proxy register with an internet service provider to select an IP address of the first network and provide the IP address of the first network to said one of the plurality of

15   workstations.

8.   The system as recited in claim 6 wherein the second device is adapted to initially handshake with an address server to assign an IP address of the second network to a user device and is adapted to handshake with a registration server to proxy register with an internet

20   service provider to select an IP address of the first network and replace the IP address of the user device with the IP address of the first network.

9.   The system as recited in claim 1 further comprising:

            a user device connected to the second device, the user device

25   being assigned a unique IP addresses from the first network, the user device connected to a local network, the local network being assigned a set of non-unique IP addresses, the user device adapted for performing network address translation from the local network to the corresponding first network.

10. A system comprising:

a first device for receiving a datagram from a public network whose destination is specified by a globally unique Internet Protocol (IP) address and for mapping said globally unique IP address to a non-

5   globally unique IP address in a private network; and

a second device for routing said datagram to a user device connected to the second device wherein said user device includes the destination specified by said non-globally unique IP address and for mapping said non-globally unique IP address to said corresponding

10   globally unique IP address.

11. The system as recited in claim 10 wherein each mapping device comprises means for performing basic network address translation.

12. The system as recited in claim 10 comprising a local network connected to the user device, the user device being assigned a globally

15   unique IP addresses, the user device connected to a local network, the local network being assigned a set of non-unique IP addresses, the user device adapted for performing network address translation from the local network to the corresponding public network.

13. The system as recited in claim 10 wherein the second device,

20   with a connection to the user device initially having an IP address of the private network, is adapted to handshake with a registration server to proxy register with an internet service provider to select an IP address of the public network and provide the IP address of the public network to said user device.

25   14. The system as recited in claim 10 wherein the second device is adapted to initially handshake with an address server to assign an IP address of the private network to a user device and is adapted to handshake with a registration server to proxy register with an internet service provider to select an IP address of the public network and

28

replace the IP address of the user device with the IP address of the public network.

15.   The system as recited in claim 10 comprising computer readable program code comprising:

5   a first computer readable program code for causing a computer to receive the datagram from the Internet whose destination is specified by the globally unique Internet Protocol (IP) address and for causing the computer to map said globally unique IP address to the non-globally unique IP address; and

10   a second computer readable program code for causing a computer to receive the datagram whose destination is specified by the non-globally unique Internet Protocol (IP) address and for causing the computer to map said globally non-unique IP address to the corresponding globally unique IP address.

15 16.   A system for performing network address translation comprising:

           a first device for connecting to a public network, said public network including a globally unique Internet Protocol address, said first device capable of performing network address translation from the

20 globally unique Internet Protocol address to a non-globally unique Internet Protocol address; and

           a second device for connecting a user device to the public network, said second device capable of performing network address translation from the non-globally unique Internet Protocol address to

25 the corresponding globally unique Internet Protocol address.

17.   The system as recited in claim 16 wherein the second device, with a connection to the user device initially having an IP address of

the private network, is adapted to handshake with a registration server to proxy register with an internet service provider to select an IP address of the public network and provide the IP address of the public network to said user device.

5   18.   The system as recited in claim 16 wherein the second device is adapted to provide an IP address of the private network to a user device and is adapted to handshake with a registration server to proxy register with an internet service provider to select an Internet Protocol address of the public network and replace the Internet Protocol address of the

10   user device with the Internet Protocol address of the public network.

19.   The system as recited in claim 16 comprising a local network connected to the user device, the user device being assigned a globally unique Internet Protocol addresses, the user device connected to a local network, the local network being assigned a set of non-unique Internet

15   Protocol addresses, the user device adapted for performing network address translation from the local network to the corresponding public network.

20.   The system as recited in claim 16 wherein the first device and second device is adapted to eliminate a need for inspection and possible

20   modification of IP datagram data content when translating addresses in the IP datagram header.

21.   The system as recited in claim 16 wherein the first device and second device is adapted to allow arbitrary end-to-end IP datagram encryption and authentication arrangements to inter-operate between

25   public networks separated by a shared private network.

22.   The system as recited in claim 16 wherein the second device is adapted to use non-globally unique IP addresses to collectively deliver content to a plurality of user devices.

23.   The system as recited in claim 16 comprising a content server adapted to use non-globally unique IP addresses to collectively deliver content to a plurality of user devices.

24.   The system as recited in claim 16 wherein the second device is adapted to selectively assigning a non-globally unique IP address when connectivity to only a non-unique address network is required and a globally unique IP address when connectivity to networks requiring unique addressing is required.

25.   A system for performing network address translation comprising:

a first device for connecting a first private network to a public network, said public network including a globally unique Internet Protocol address, said first device capable of performing network address translation from a non-globally unique Internet Protocol address of the first network to a globally unique Internet Protocol address; and

a second device for connecting a second private network using non-globally unique Internet Protocol addresses to the public network, said second device capable of performing corresponding network address translation from a non-globally unique Internet Protocol address of the second network to a globally unique Internet Protocol address, the first device and the second device communicating with each other to provide a contiguous single network between the first private network and the second private network.

31

26.   A computer program product comprising a computer usable medium having computer readable program code embodied in said medium for causing an application program to execute on a computer that performs network address translation, said computer readable

5   program code comprising:

a first computer readable program code for causing a computer to receive a datagram from the Internet whose destination is specified by a globally unique Internet Protocol (IP) address and for causing the computer to map said globally unique IP address to a non-globally

10   unique IP address; and

a second computer readable program code for causing a computer to receive a datagram whose destination is specified by a non-globally unique Internet Protocol (IP) address and for causing the computer to map said globally non-unique IP address to the

15   corresponding globally unique IP address.

1/8

100

E.G., CUSTOMER LAN   E.G., FIXED WIRELESS   E.G., PUBLIC INTERNET

FIRST
NETWORK

SECOND
NETWORK

THIRD
NETWORK

2   20   4   30   6

CAN SKIP THIS STEP
BECAUSE SECOND
NETWORK DOES NOT
REQUIRE S TO BE A
'NATIVE' ADDRESS TO
FORWARD TRAFFIC TO
THIRD NETWORK

D ◄— D'   D'◄— D
S —► S'   S' —► S

KEY:

D= DESTINATION ADDRESS IN IP DATAGRAM
S= SOURCE ADDRESS IN IP DATAGRAM
[D,S]= GLOBALLY UNIQUE IP ADDRESSES
[D',S']= NON GLOBALLY UNIQUE IP ADDRESSES
☐ = OPTIONAL STEP

ASSUMPTIONS:

- FIRST NETWORK AND
THIRD NETWORK USE
GLOBALLY UNIQUE ADDRESS

- SECOND NETWORK USES
NON GLOBALLY UNIQUE
ADDRESSES

FIG. 1

FIG. 1A

100

THE INTERNET
50

40′   S=24.128.225.93
     D=216.41.29.6

SERVICE PROVIDER
(ISP)
40

40″   S=216.41.29.6
     D=24.128.225.93

30′   S=10.0.0.93
     D=216.41.29.6

PRIVATE NETWORK
ROUTER
30

30″   S=216.41.29.6
     D=10.0.0.93

20′   S=10.0.0.93
     D=216.41.29.6

PRIVATE NETWORK
ROUTER
20

20″   S=216.41.29.6
     D=10.0.0.93

10′   S=24.128.225.93
     D=216.41.29.6

USER DEVICE
IP=24.128.225.93
10

10″   S=216.41.29.6
     D=24.128.225.93

FIG. 2

FIG. 3

FIG. 3A

HLAN   BASE NETWORK   DSN

PC   RU   S&P SERVER (DHCP)   REGISTRATION SERVER   BR (NAT)

DHCP (DISCOVER) → RELAY DHCP (DISCOVER) →

MAC= ? (NEW DEVICE, FAILED LOOKUP)
DEVICE & RU NOT REGISTERED
ASSIGN SERVICE="NEW USER"
DERIVE IP ADDRESS FROM STATIC RU POOL
10.0.0.1 RU, MAC XXXXX
10.0.0.2 DEVICE, MAC YYYYY

DHCP (OFFER) ← RELAY DHCP (OFFER) ←

DHCP (REQUEST) → RELAY DHCP (REQUEST) →

DHCP (ACK) ← RELAY DHCP (ACK) ←

PRIVATE ADDRESS ALLOWS USER TO ACCESS
FWS INTERNAL NETWORK BUT NOT EXTERNAL
(NO NAT POOL ASSIGNED YET)

HTTP REGISTRATION SESSION BEGIN

REGISTRATION SESSION WITH
SERVER. USER SELECTS ISP "ISP1"
GoS "Gold", BILLING METHOD

PROXY AAA USER WITH EXTERNAL
ISP SERVERS (COULD BE
INDEPENDENT PROCESS)

10.0.0.2 DEVICE, MAC YYYYY
QoS=HIGH
DNS=YES

SNMP SET (10.0.0.2="ISP1/Gold")

SNMP SET (10.0.0.2="ISP1/Gold")

"ISP1/Gold POLICY" NAT GROUP 1
QoS HIGH   DNS=YES

LDAP LOOKUP OF "ISP1/Gold"

LDAP RESPONSE OF "ISP1/Gold"

CHOOSE PUBLIC IP
FROM NATI POOL
ADD NAT ENTRY
10.0.0.2=
130.42.61.7

10.0.0.2 PRIVATE
130.42.61.7 PUBLIC
MAC YYYYY
QoS=HIGH
DNS=YES

ADD NAT ENTRY
10.0.0.2 =
130.42.61.7

SNMP SET (10.0.0.2=130.42.61.7)

SNMP SET (10.0.0.2=130.42.61.7)

REGISTRATION SESSION WITH
SERVER ENDS. USER INSTRUCTED
TO REBOOT THEIR PC

HTTP REGISTRATION SESSION END

FIG. 4

FIG. 5

CHOOSE PULBIC IP FROM
NAT1 POOL
ADD NAT ENTRY
10.0.0.3=130.42.14.25

DSN

BR (NAT)

REGISTRATION SERVER

SNMP SET
(10.0.0.3=130.42.14.25)

MAC= ? (UNRECOGNIZED)
DEVICE UNREGISTERED, RU REGISTERED

SERVICE= "ISP1/Gold"
10.0.0.3 DEVICE, MAC ZZZZZZ

SNMP SET
(10.0.0.3 = "ISP1/Gold")

PUBLIC ADDRESS ALLOWS USER TO
ACCESS FWS EXTERNAL NETWORK

BASE NETWORK

S&P SERVER (DHCP)

RELAY DHCP (DISCOVER)

10.0.0.3 PRIVATE,
130.42.14.25 PUBLIC
MAC ZZZZZZ
QoS = HIGH
DNS = YES

ADD NAT ENTRY
10.0.0.3=130.42.14.25

SNMP SET
(10.0.0.3 = 130.42.14.25)

RELAY DHCP (OFFER)

RELAY DHCP (REQUEST)

RELAY DHCP (ACK)

HLAN

RU

(USER APPLIANCE TURNS ON...)

DHCP (DISCOVER)

DHCP (OFFER)

DHCP (REQUEST)

DHCP (ACK)

PC

200

E.G., PRIVATE INTRANET   E.G., PUBLIC INTERNET   E.G., PRIVATE INTRANET

FIRST NETWORK   120   SECOND NETWORK   130   THIRD NETWORK

110   102   2   104   1   106   140

THIS IS A SCENARIO WHERE TWO PRIVATE NETWORKS WISH TO COMMUNICATE ACROSS A PUBLIC NETWORK WHILE TRANSPARENTLY (TO END STATIONS) USING PRIVATE NETWORK ADDRESSES

S' ← S   S ← S'
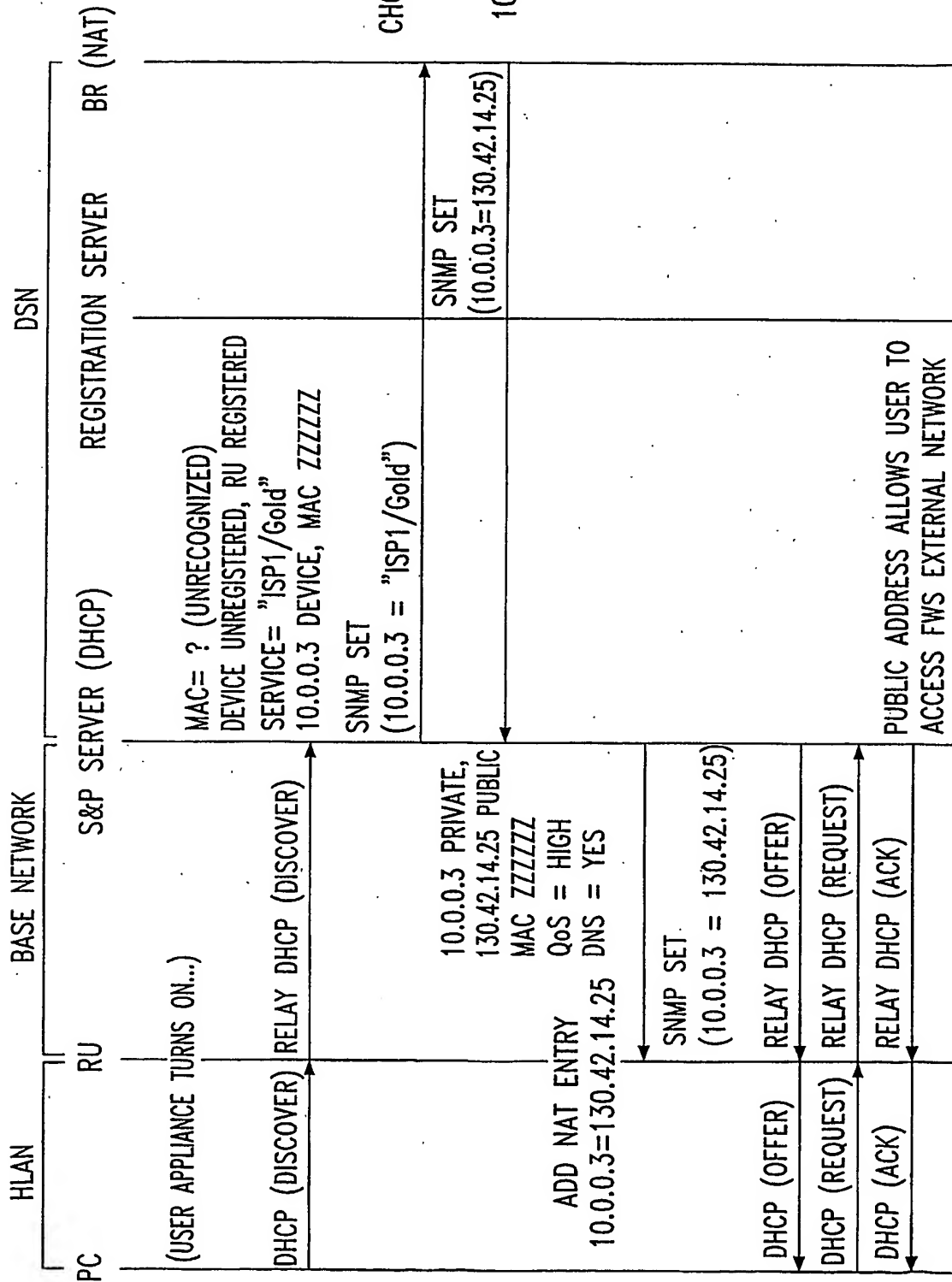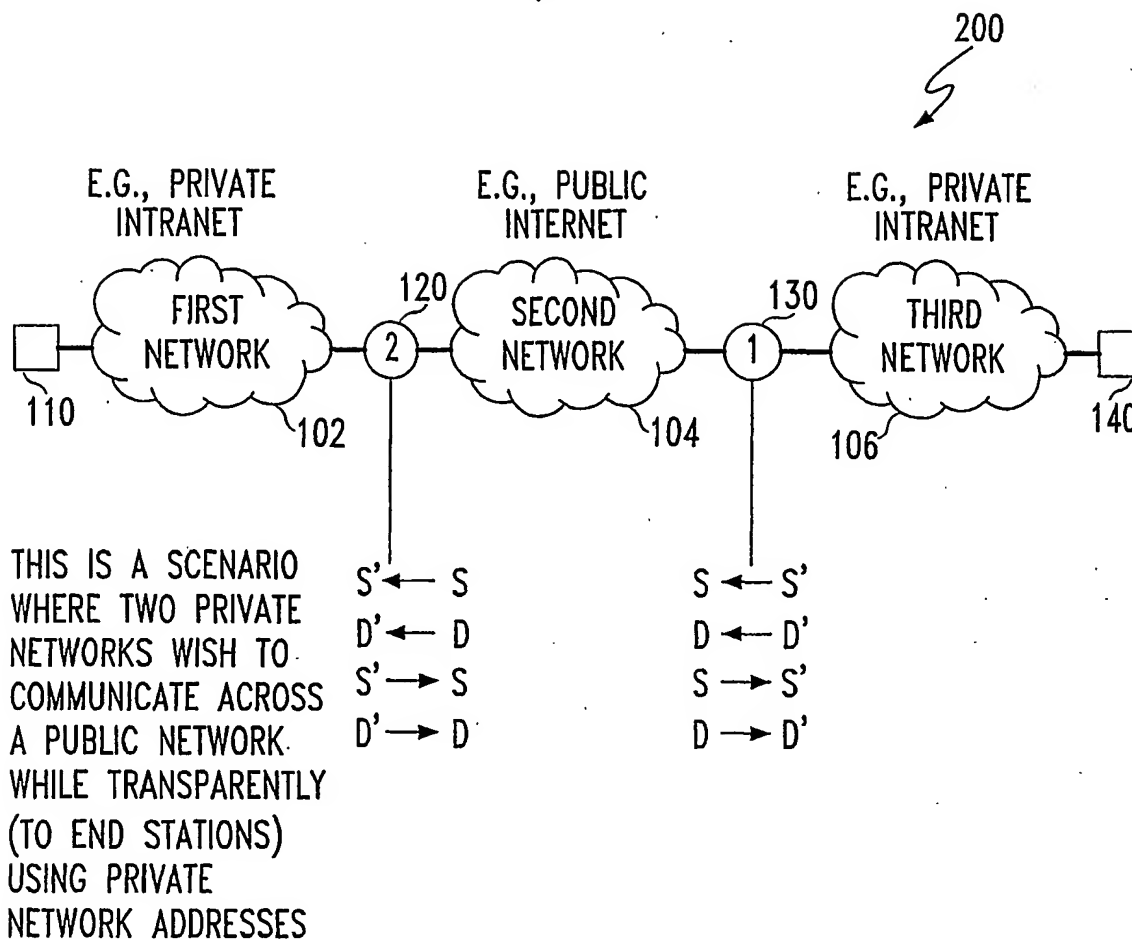D' ← D   D ← D'
S' → S   S → S'
D' → D   D → D'

KEY:

D= DESTINATION ADDRESS IN IP DATAGRAM
S= SOURCE ADDRESS IN IP DATAGRAM
[D,S]= GLOBALLY UNIQUE IP ADDRESSES
[D',S']= NON GLOBALLY UNIQUE IP ADDRESSES

ASSUMPTIONS:

– FIRST NETWORK AND THIRD NETWORK USE NON GLOBALLY UNIQUE ADDRESS

– SECOND NETWORK USES GLOBALLY UNIQUE ADDRESSES

FIG. 6